International Journal of Computer Science Engineering
and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 3, Issue 5, Dec 2013, 11-18
© TJPRC Pvt. Ltd.

IMAGE ENCRYPTION USING HENON CHAOTIC MAP WITH BYTE SEQUENCE

N. S. RAGHAVA & ASHISH KUMAR

Department of Information Technology, Delhi Technological University, New Delhi, India

ABSTRACT

Communication is a meaningful exchange of information between two or more entities. In this era of e-communication i.e. the transmission of non-physical data that has been encoded digitally for the purpose of storage and processing of information, the first concern is about the security of the content which is shared during communication. Security is a continuous process via which data can be secured from several active and passive attacks. Encryption technique protects the confidentiality of a message or information which is in the form of multimedia (text, image, and video).

In this paper, a new symmetric image encryption algorithm is proposed based on Henon's chaotic system with byte sequences applied with a novel approach of pixel shuffling of an image which results in an effective and efficient encryption of images. By increasing confusion and diffusion, statistical analysis and experimental analysis of key sensitivity proved that the proposed image encryption algorithm resulted in a new dimension for secure image transfer in digital transmission world.

KEYWORDS: Cryptography, Chaotic System, Henon Map, Confusion and Diffusion

INTRODUCTION

Multimedia is defined as the field that deals with different forms of information such as text, images, audio and videos in an integrated fashion [1]. Now-a-days digital images are used frequently for communication. Any information shared over Internet needs high level of protection from intruders [2].

Cryptography [3][4] is the art of protecting information by transforming readable information (plain data) into unreadable format (cipher) with the help of well-structured encryption algorithms and secret keys. Cryptography scheme is of two types. One is known as symmetric key cryptography [5] in which a single secret key is used for both, encryption at sender's end and decryption at receiver's end.

The other scheme known as public key cryptography system is based on asymmetric key cryptography in which each host has a pair of keys i.e. a public key which is known to every other host in communication and a private key which is not disclosed to any other host. In past few decades, chaotic signal [6] [7] is widely used in cryptography system. Chaos is a Greek word which means unpredictable and studied under the non-linear dynamic system. Chaotic systems are popular for their randomness and non-predictable behaviour.

CHAOS THEORY AND HENON MAP

Edward Lopez derived a Chaos theory which is a part of mathematical physics. A chaotic system based on confusion and diffusion was developed in 1989 [8]. Chaotic systems are sensitive, non-liner, deterministic and easy to reconstruct after filling in the image. Henon map is one of the chaotic map used for generating Pseudo-random sequence required for encryption.

Henon chaotic map [9-10] discovered in 1978 is used as a symmetric key stream cipher cryptographic system. It is mathematical in nature. Two dimensional discrete-time nonlinear dynamical Henon chaotic map generates pseudo-random binary sequence which has been described as below

$$X_{n+1} = 1+Y_n - aX_n^2$$
$$Y_{n+1} = bX_n \quad n=0, 1, 2... \tag{1}$$

Here, the parameters, a and b are prime importance as the dynamic behaviour of system depends on these values. The system cannot be chaotic unless the value of a and b are 1.4 and 0.3 respectively. For other values of a and b, the map behaves as chaotic, intermittent, or obtain a periodic orbit. Initial points X1 and Y1 [11] work as a symmetric key for chaotic cryptographic system used for encryption at sender's end and decryption at receiver's end. Since Henon map is deterministic so decryption of the cipher image will reconstruct the original image at receiver's end with the same initial points X1 and Y1. Thus, sensitivity of key and encryption algorithm together contributes to avoid all kind of cryptanalysis attacks [2].

$$X_{n+1} = 1+Y_n - 1.4X_n^2$$
$$Y_{n+1} = 0.3X_n \tag{2}$$

RELATED WORK

The most popular symmetric key cryptography is DES (data encryption algorithm) [12]. It is the name of federal information processing standard (FIPS) 46-3; it shows DEA originated in IBM .it was adopted in 1977 as a standard by US Government for all commercial and unclassified information. In the last decade, chaotic systems are actively working in symmetric key cryptography system.

In [13], Chen at el. presented symmetric image encryption scheme based on 3D chaotic cat maps. Wang at el. In [14], a 3D Cat map based symmetric image encryption method is introduced. Combined image encryption algorithm based on diffusion mapped disorder and hyper chaotic systems encryption scheme are also presented in [15][16]. However, the encryption arithmetic based on 3D chaotic cat maps has a non-independent key space and is a computationally expensive process.

Chen Wei-bin and Zhang Xin [17] proposed an image encryption algorithm based on Arnold cat map with Henon chaotic system. Firstly, Arnold cat map is used to shuffle image pixels and then Henon map is used for encryption pixel by pixel. In paper [18], a survey has been done on various image encryption methodology on which reveals the chaotic system.

PROPOSED ENCRYPTION ALGORITHM USING HENON MAP

The inputs to the chaotic Henon system are the image to be encrypted and the initial values of Henon map which are treated as a key. In this paper, I denote an image of size m×n.

Shuffling of Image

Shuffling is useful to disturb the correlation among the adjacent pixel. Shuffling of the image depends upon the number of rows and columns. Here, shuffling of pixel is done in two steps.

Step 1: With each iteration, a quadrant is subdivided into sub-quadrants.

Step 2: For the kth iteration, if it is odd then shuffling of quadrant is in clockwise direction otherwise anti-clockwise direction. To illustrate, two iterations are represented in figure.2.

First Iteration

Initially, divide the image in four quadrants and then rotate each quadrant in clockwise direction. As a shown in figure 1, TL shifts to TR position, TR shifts to BR position, BL shifts to TL position and last quadrant of image BR shifts to BL position.

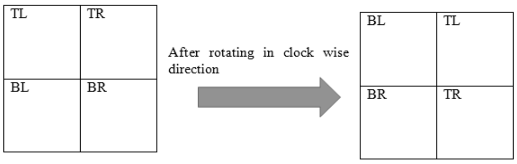
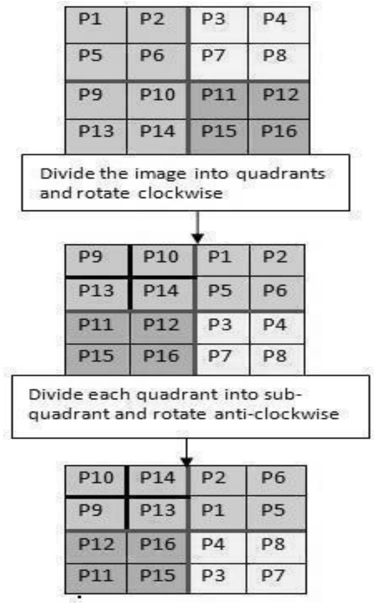


Figure 1: Image Shuffling after First Iteration

Second Iteration

Now each quadrant of shuffled image obtained after first iteration is further divided into sub-quadrant and follows the same procedure which is illustrate in Figure. 1 but in anti-clock wise direction.



P1	P2	P3	P4
P5	P6	P7	P8
P9	P10	P11	P12
P13	P14	P15	P16

Divide the image into quadrants and rotate clockwise

P9	P10	P1	P2
P13	P14	P5	P6
P11	P12	P3	P4
P15	P16	P7	P8

Divide each quadrant into sub-quadrant and rotate anti-clockwise

P10	P14	P2	P6
P9	P13	P1	P5
P12	P16	P4	P8
P11	P15	P3	P7

Figure 2: Shuffled Image after Two Iterations

Image Encryption by Henon Chaotic System

The shuffled image is encrypted using pseudo-random binary sequence generated by taking key values for Henon map.

Step 1: choose the initial value of (X1,Y1) for Henon map. This value works as an initial secret symmetric key for Henon map.

Step 2: Henon map work as a key stream generator for cryptosystem. The size of sequence depends upon the size of image. If the image size is m×n then the number of henon sequence will be 8×m×n obtained by equation (2).

Step 3: Experimental analysis conclude [11] that cut-off point, 0.3992, has been determined so that the sequence is balanced. The decimal values are then converted into binary values depending upon this threshold value as given in eqaution (3) where Z is a binary sequnce.

.
$$Z_i = \begin{cases} 0 \text{ if } Xi \leq 0.3992 \\ 1 \text{ if } Xi \geq 0.3992 \end{cases} \quad (3)$$

Step 4: Henon sequence is then reduced by combining each consecutive 8 bits into one decimal value.

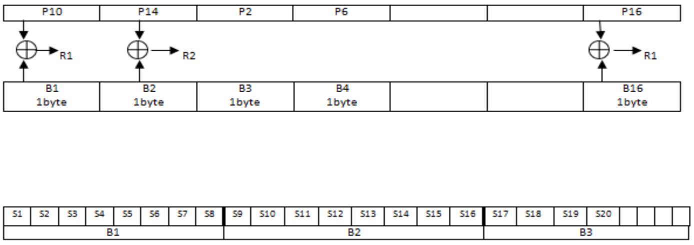


Figure 3: Encryption with Byte Sequence

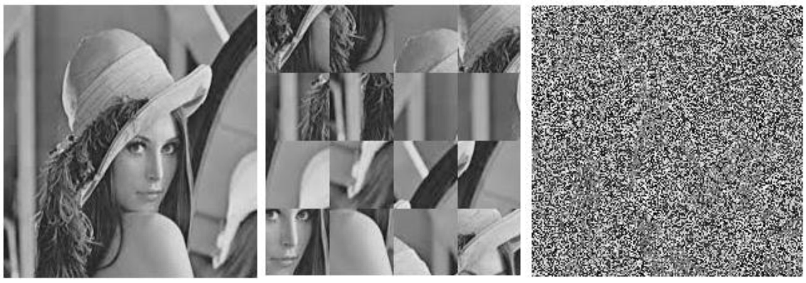
Step 5: Encryption is done by bitwise Exclusive-OR operation between shuffled image and sequence generated in step 4.

Decryption of Encrypted Image

Since, the chaotic system behaviour is deterministic so reconstruction of image using the same key (X_1, Y_1) at decryption end gives the shuffled image. This shuffled image is further arranged in an order exactly opposite of the way done for encryption as mentioned in section III (A). Finally, the original image is obtained at receiver's end.

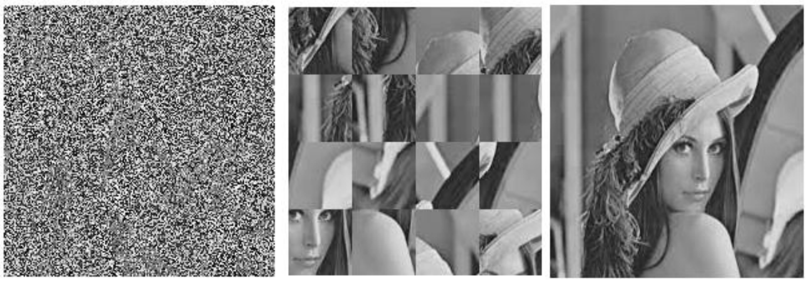
EXPERIMENTAL RESULTS AND DISCUSSIONS

In this section, experimental results of the proposed image encryption algorithm are illustrated to appreciate the efficiency of proposed algorithm. The MATLAB 7.9 software was used for implementing this code. Here, test image of size 204×204 is shown in Figure 4(a). The initial parameters for Henon map are chosen as a=1.4 and b=0.3 to make the system chaotic. Secret symmetric key for encryption is a combination of X1=0.01 and Y1=0.02. Figure 4(b) and Figure 4(c) illustrates shuffled image after two iterations and encrypted image respectively.



(a) **(b)** **(c)**

Figure 4: Encryption by Henon Chaotic System: (A) Original Image; (B) Shuffled Image; (C) Cipher Image

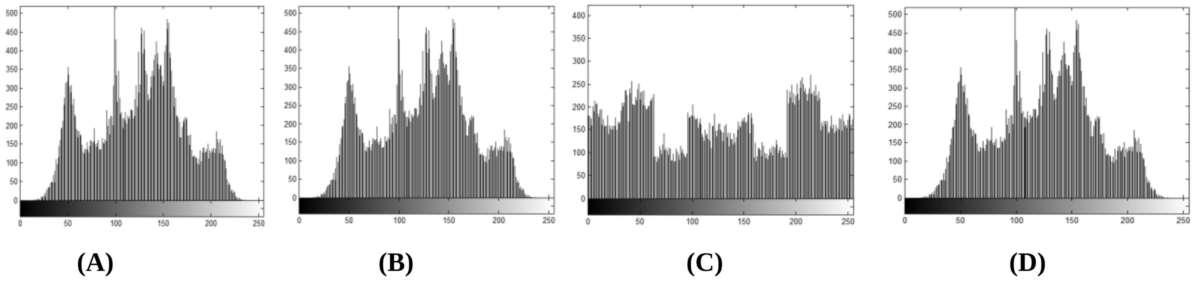


(a) **(b)** **(c)**

Figure 5: Decryption by Henon Chaotic System: (A) Cipher Image; (B) Shuffled Image After Decryption; (C) Original Image

Histogram Analysis

The histogram of an image is graphical representation of pixel intensity values. There are 256 different possible intensities for a gray image, so in graphical representation of the histogram will display 256 intensities and the distribution of pixels amongst those intensity values.



(A) (B) (C) (D)

Figure 6: Histogram Analysis: (A) Histogram of Original Image; (B) Histogram of Shuffled Image; (C) Histogram of Cipher Image; (D) Histogram of Decrypted Image

It is analysed from Figure 6, that the distribution of gray scale values is uniform in cipher image, and significantly different from histograms of original image.

In the original image some gray scale values do not exist in the range of 0 to 255 but in encrypted image gray-scale values exist uniformly in the range 0 to 255. Therefore, it is proved that the encrypted image does not help intruders to employ statistical attack on encryption procedure.

Information Entropy Analysis

Information entropy is defined by the degree of uncertainties in the encryption system. It is used to calculate the Effectiveness of image encryption algorithm. Statistical measure of randomness to characterize the texture of the input image is termed as entropy. It is calculated as given in equation (4).

H= -sum (p.*log2 (p)) (4)

Ideal entropy of an encrypted image should be equal to 8, which corresponds to a random source. Practically, ideal information entropy cannot be achieved. It is always less than the ideal value. The values calculated in Table 1 are very close to the ideal value.

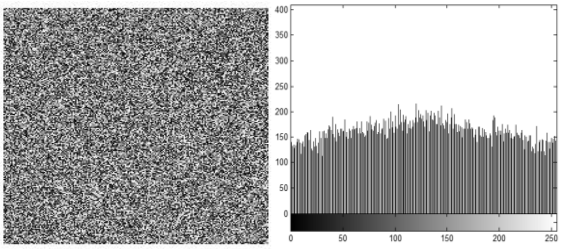
Table 1: Entropy Analysis

	Original Image	After First Iteration	After Second Iteration
Entropy	7.4521	7.9406	7.9383

Key Sensitivity Test

For secure encryption, the key should be sensitive with large space key size to resist all kind of brute force attack. Randomness is the key point of Henon map.

To test the sensitivity of the key involved, a minute variation was done in original secret key by changing it from x(1)=0.01 and y(1)=0.02 to x’(1)=0.010001 and y’(1)=0.020001. As a result, it was not possible to obtain the original image at receiver’s end.



(a) (b)

Figure 7: Key Sensitivity Analysis: (a) Decrypted Image after Slight Variation in Key; (b) Histogram of Decrypted Image

CONCLUSIONS

The proposed method was applied to a test image and results thus obtained proved a higher level of security of images. Eavesdrop cannot cryptanalysis the cipher image. Here, the security relies on a secret key along with the image encryption technique. Chaos is known for randomness, so it is highly secured. Confusion has been done by pixel movement form actual position to a new position and diffusion has been done through byte sequence generated through Henon map. So both the processes of increasing confusion and diffusion resulted in increasing the security of cryptosystem.

REFERENCES

1. Susanne Boll, “MultiTube–Where Multimedia and Web 2.0 Could Meet,” *IEEE Computer Society,* 2007.
2. Jiri Giesl, Kerel Vlcek, Ladislav Behal, “Improving Choas Image Encryption Speed,” *International Journal of Future Generation Communication and Networking,* 2009.
3. G. Chen, Y. Mao, C.K. Chui, “A symmetric image encryption scheme based on 3D chaotic cat maps,” *Chaos Solitons Fractals 21* (2004) 749-761.
4. S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, A. Akhavan, “A fast chaotic encryptions cheme based on piece wise nonlinear chaotic maps,” *Physics Letters,* A, 366 (2007) 391–396.
5. G. Jakimoski, L. Kocarev, “Block encryption ciphers based on chaotic maps,” *IEEE Transaction on Circuits System-I.* 48 (2002) 163-169.
6. G. Jakimoski and L. Kocarev., “Analysis of recently proposed chaos-based encryption algorithm,” *Physics Letters*,A,2001.
7. A.T.Parker and K.M.Short, “Reconstructing the keystream from a chaotic encryption scheme,” *IEEE transaction on circuit and systems-I*,485(5),2001.
8. Matthews R., “On the derivation of a chaotic encryption algorithm,” *Cryptologia* 1989;8(1):29–41.
9. E. Petrisor, “Entry and exist sets in the dynamics of area preserving Henon map,” *Chaos, Solitions and Fractals*, pp.651-658, Oct 2003
10. L. Guo, Z. Shi-ping, X. De-ming, L. Jian-wen, “An Intermittent Linear Feedback Method for controlling Henon-like Attractor,” *Journal of Applied Science,* pp. 288-290, Dec.2001.
11. D.Erdmann and S. Murphy, “HENON STREAM CIPHER,” *electronics Letters 23rd april 1992 vol. 28 no.9*

12. Miles E. Smld And Dennis K. Branstad, "The Data Encryption Standard: Past and Future," *PROCEEDINGS OF THE IEEE, VOL. 76, NO. 5, MAY 1988.*

13. G. Chen, Y. Mao, K. Charles, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solutions & Fractals*, pp. 749-761, Dec. 2004.

14. K. Wang, W. Pei, "On the security of 3D Cat map based symmetric image encryption scheme," *Physics Letters A.*, pp. 432-439, May. 2005.

15. S.-M. Chang, M.-C. Li, W.-W. Lin, "Asymptotic synchronization of modified logistic hyper-chaotic systems and its applications," *Nonlinear Analysis, pp. 869–880, Jan. 2009.*

16. H. Lian-xi, L. Chuan-mu, L. Ming-xi, "Combined image encryption algorithm based on diffusion mapped disorder and hyperchaotic systems," *Computer Applications, pp. 1892-1895, Aug. 2007.*

17. Chen Wei-bin, Zhang Xin, "Image Encryption Algorithm Based on Henon Chaotic System," 978-1-4244-3986-7/09/$25.00 ©2009 IEEE.

18. **M**intu Philip, Asha Das, "Survey: Image Encryption using Chaotic Cryptography Schemes," *IJCA Special Issue on "Computational Science- New Dimensions & Perspectives" Nccse, 2011.*